

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-171717

(43) 公開日 平成10年(1998) 6月26日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
G 0 6 K 17/00		G 0 6 K 17/00	E
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A
9/10			6 0 1 B
			6 0 1 E

審査請求 未請求 請求項の数 3 O L (全 8 頁) 最終頁に続く

(21) 出願番号 特願平8-324942

(22) 出願日 平成8年(1996)12月5日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 高木 伸哉

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 梅原 紀夫

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

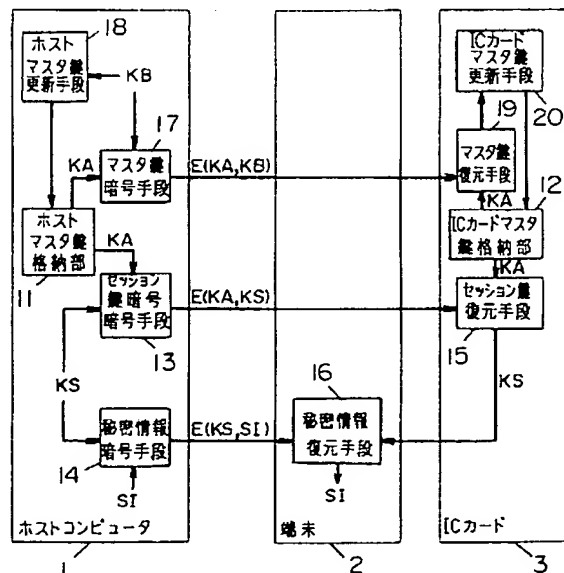
(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 ICカードおよびそれを用いた暗号通信システム

(57) 【要約】

【課題】 ホストコンピュータと端末間で通信される暗号化データを盗聴され、かつ暗号鍵を管理するICカードが盗まれても安全な暗号通信システムを提供する。

【解決手段】 ホストコンピュータ1は現在のマスター鍵Mによって新しいマスター鍵Nを暗号化しICカード3に送る。ホストコンピュータ1とICカード3は、マスター鍵によりセッション鍵を暗号化して配送する毎に、自身のマスター鍵Mを新しいマスター鍵Nに更新する。これにより、セッション鍵およびそれによって暗号化された秘密情報の解読を防ぐことができる。



【特許請求の範囲】

【請求項1】 暗号通信に用いるマスタ鍵Nもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Mを格納するICカードマスタ鍵格納部と、外部から受信した暗号化されたマスタ鍵Nデータを復号化して、マスタ鍵Nを復元するマスタ鍵復元手段と、現在のマスタ鍵Mもしくはマスタ鍵Nを用いて外部から受信した暗号化されたセッション鍵データを復号化して、暗号通信を行う度にランダムに生成されるセッション鍵を復元するセッション鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ICカードマスタ鍵格納部に格納されている現在のマスタ鍵Mをマスタ鍵Nに更新するICカードマスタ鍵更新手段とを備えたことを特徴とするICカード。

【請求項2】 ICカードマスタ鍵格納部に格納されているマスタ鍵Mを用いて、外部から受信した暗号化されたセッション鍵データを復号化し、セッション鍵を復元し、外部へ送信するセッション鍵復元手段と、セッション鍵の復元後に前記ICカードマスタ鍵格納部に格納されているマスタ鍵Mを用いて、外部から受信した暗号化されたマスタ鍵Nデータを復号化するマスタ鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ICカードマスタ鍵格納部に格納されている現在のマスタ鍵Mをマスタ鍵Nに更新するICカードマスタ鍵更新手段とを備えたことを特徴とする請求項1記載のICカード。

【請求項3】 ホストコンピュータと、前記ホストコンピュータに接続される端末と、前記端末に着脱可能な状態で接続されるICカードとを有し、前記ホストコンピュータは、マスタ鍵Nもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Mを格納するホストマスタ鍵格納部と、前記ホストコンピュータにおいて新たに生成したマスタ鍵Nを暗号化して、マスタ鍵Nデータを送信するマスタ鍵暗号手段と、暗号通信を行う度にランダムに生成されるセッション鍵を暗号化してセッション鍵データを送信するセッション鍵暗号手段と、秘密情報を暗号化して秘密情報データを送信する秘密情報暗号手段と、前記ホストマスタ鍵格納部に格納されている現在のマスタ鍵Mをマスタ鍵Nに更新するホストマスタ鍵更新手段とを備え、

前記ICカードは、マスタ鍵Mを格納するICカードマスタ鍵格納部と、外部から受信したセッション鍵データを復号化して、セッション鍵を復元し、前記端末にセッション鍵を送信するセッション鍵復元手段と、外部から受信したマスタ鍵Nデータを復号化して、マスタ鍵Nを復元するマスタ鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ICカードマスタ鍵格納部に格納されている現在のマスタ鍵Mをマスタ鍵Nに更新するICカードマスタ鍵更新手段とを備え、

前記端末は、前記ICカードから受信したセッション鍵

を用いて、前記ホストコンピュータから受信した秘密情報データを復号化して、秘密情報を復元する秘密情報復元手段を備えた暗号通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はマイクロプロセッサとメモリを内蔵し、ICカード使用者の正当性確認、マスタ鍵Mの保管用等を使用されるICカードおよびそれを用いた暗号通信システムに関する。

【0002】

【従来の技術】ホストコンピュータと端末間で暗号通信を行う際、安全性を高めるため暗号通信に用いる鍵を毎回変えることが望ましい。このために、鍵を暗号化するためのマスタ鍵Mを双方で共有し、これを用いて、実際の暗号通信に使用されるマスタ鍵Nもしくはセッション鍵を暗号化して秘密暗号鍵として安全に配送する。この実際の暗号通信に使用される鍵であるセッション鍵は、その場限りに使用される鍵として、暗号通信を行う度にランダムに生成される。

【0003】従来の暗号通信システムについて、図3を用いて説明する。図3では、ホストコンピュータ101と端末102間で秘密暗号鍵を用いて暗号通信を行う場合を示している。ホストコンピュータ101はホストマスタ鍵格納部111にマスタ鍵M・KMを有している。もう一方のマスタ鍵M・KMを端末102内に格納すると、不正者により端末102に格納されているマスタ鍵M・KMが盗まれる可能性があるため、物理的に安全な、すなわち内部のデータを不正に外から読み書きすることができないICカード103のICカードマスタ鍵格納部112内に格納されている。

【0004】以下に暗号通信の流れを示す。まずホストコンピュータ101はセッション鍵KSをランダムに生成する。第1の暗号手段113は、ホストマスタ鍵格納部111に格納されているマスタ鍵M・KMによりセッション鍵KSを暗号化したセッション鍵データE(KM, KS)を、端末102を介してICカード103に送る。ICカード103の第1の復元手段114は受信したセッション鍵データE(KM, KS)を、ICカードマスタ鍵格納部112に格納されているマスタ鍵M・KMにより復号化してセッション鍵KSを復元し、これを端末102へ送る。

【0005】これにより、ホストコンピュータ101と端末102は同じセッション鍵KSを共有したこととなり、このセッション鍵KSを用いて秘密情報S1の暗号通信を行う。具体的には、ホストコンピュータ101の第2の暗号手段115がセッション鍵KSにより本来通信すべき情報である秘密情報S1を暗号化した秘密情報データE(KS, S1)を生成して端末102に送り、端末102の第2の復元手段116がこの秘密情報データE(KS, S1)をICカード103より送られてき

たセッション鍵KSにより復号化し、秘密情報SIを復元する。

【0006】ここで、第2の復元手段116による処理は端末102内で行うよりも、物理的に安全なICカード103内で行う方がセキュリティは高くなるが、ICカード103は処理能力に限界があるため、秘密情報SIが長い電文である場合等は復号化に時間がかかる。そのため、暗号化された秘密情報SIの復号処理は端末102内で行い、ICカード103は鍵の管理、すなわちマスタ鍵M・KMの保管およびセッション鍵KSの復元のみを行っている。

【0007】従って、例えば端末102とICカード103が通信を行う時は、ICカード103が端末102内に取り込まれる等、端末102とICカード103間の通信は安全であることが必要である。しかしながら実際には、端末102とICカード103がケーブル等で接続される場合であっても、その間の通信を盗聴できる者は限定されるため、比較的安全である。

【0008】

【発明が解決しようとする課題】ところが、ホストコンピュータと端末間の通信には公衆回線を使用する場合が多く、この間を伝送されるデータ、すなわちセッション鍵データE(KM, KS)および秘密情報データE(KS, SI)は容易に盗聴され得る。これらはいずれも暗号化されているため、それだけで秘密情報が洩れる心配はないが、盗聴した不正者が更にICカードを盗んだ場合、盗聴したセッション鍵データE(KM, KS)を盗んだICカードに入力すれば、第1の復元手段がこれを復号化してセッション鍵を外部に出力するため、不正者はセッション鍵を知ることができる。従って、不正者はセッション鍵と盗聴した秘密情報データE(KS, SI)とから秘密情報を知ることができるという問題点があった。

【0009】通常、ICカードは盗まれても使用できないよう使用者自身の設定した暗証番号でロックをかけているが、暗証番号は誕生日など簡単な数値の組み合わせにしている使用者も多く、第3者に知られやすいものであり、安全であるとは言えない。

【0010】本発明はこのような問題点を解決するために、ホストコンピュータと端末間で通信される暗号化データを盗聴され、かつ鍵を管理するICカードが盗まれても安全なICカードおよびそれを用いた暗号通信システムを提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するために本発明のICカードは、暗号通信に用いるマスタ鍵Nもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Mを格納するICカードマスタ鍵格納部と、外部から受信した暗号化されたマスタ鍵Nデータを復号化し、マスタ鍵Nを復元するマスタ鍵復元手段と、現在の

マスタ鍵Mもしくはマスタ鍵Nを用いて外部から受信した暗号化されたセッション鍵データを復号化して、暗号通信を行う度にランダムに生成されるセッション鍵を復元するセッション鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ICカードマスタ鍵格納部に格納されている現在のマスタ鍵Mをマスタ鍵Nに更新するICカードマスタ鍵更新手段とを備えたものである。

【0012】また本発明の暗号通信システムは、ホストコンピュータと、前記ホストコンピュータに接続される端末と、前記端末に着脱可能な状態で接続されるICカードとを有し、前記ホストコンピュータは、マスタ鍵Nもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Mを格納するホストマスタ鍵格納部と、前記ホストコンピュータにおいて新たに生成したマスタ鍵Nを暗号化して、マスタ鍵Nデータを送信するマスタ鍵暗号手段と、暗号通信を行う度にランダムに生成されるセッション鍵を暗号化してセッション鍵データを送信するセッション鍵暗号手段と、秘密情報を暗号化して秘密情報データを送信する秘密情報暗号手段と、前記ホストマスタ鍵格納部に格納されている現在のマスタ鍵Mをマスタ鍵Nに更新するホストマスタ鍵更新手段とを備え、前記ICカードは、マスタ鍵Mを格納するICカードマスタ鍵格納部と、外部から受信したセッション鍵データを復号化して、セッション鍵を復元し、前記端末にセッション鍵を送信するセッション鍵復元手段と、外部から受信したマスタ鍵Nデータを復号化して、マスタ鍵Nを復元するマスタ鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ICカードマスタ鍵格納部に格納されている現在のマスタ鍵Mをマスタ鍵Nに更新するICカードマスタ鍵更新手段とを備え、前記端末は、前記ICカードから受信したセッション鍵を用いて、前記ホストコンピュータから受信した秘密情報データを復号化して、秘密情報を復元する秘密情報復元手段を備えたものである。

【0013】この構成により、セッション鍵を配送する毎にマスタ鍵Mを更新することとなり、盗んだICカードに不正者が盗聴した暗号化データを入力しても、もはやそのICカードのマスタ鍵Mはマスタ鍵Nに更新されており、セッション鍵を得ることはできない。従って、このセッション鍵を用いての暗号化された秘密情報の解読を防止できることとなる。

【0014】

【発明の実施の形態】以下、本発明の好ましい実施の形態について図面を参照しつつ詳細に説明する。

【0015】（実施の形態1）図1は本実施の形態における暗号通信システムの構成図であり、ホストコンピュータ1と端末2間で秘密暗号鍵を用いて暗号通信を行う場合を示している。

【0016】同図において、ホストコンピュータ1はホストマスタ鍵格納部11に現在のマスタ鍵M・KAを有

している。もう一方の復号化のためのマスタ鍵M・KAは、端末2内に格納すると端末2からマスタ鍵M・KAが盗まれる可能性があるため、物理的に安全なICカード3のICカードマスタ鍵格納部12内に格納されている。

【0017】暗号通信の手順を順を追って説明する。まずホストコンピュータ1は、セッション鍵KSをランダムに生成する。セッション鍵暗号手段13で、ホストマスタ鍵格納部11に格納されているマスタ鍵M・KAを用いてセッション鍵KSを暗号化したセッション鍵データE(KA, KS)を、端末2を介してICカード3に送信する。また秘密情報暗号手段14においては、セッション鍵KSを用いて本来通信すべき情報である秘密情報SIを暗号化した秘密情報データE(KS, SI)を端末2に送信する。

【0018】一方、ICカード3側では、セッション鍵復元手段15が受信したセッション鍵データE(KA, KS)をICカードマスタ鍵格納部12に格納されている現在のマスタ鍵M・KAにより復号化して、セッション鍵KSを復元する。復元されたセッション鍵KSは、

【0019】これにより、ホストコンピュータ1と端末2は同じセッション鍵KSを共有したこととなり、秘密情報復元手段16が受信した秘密情報データE(KS, SI)をICカード3から送信されてきたセッション鍵KSにより復号化して、秘密情報SIを復元する。そして復元された秘密情報SIにより様々な処理を行うものである。

【0020】またホストコンピュータ1はICカード3がセッション鍵を復元した後に、マスタ鍵N・KBを生成する。マスタ鍵暗号手段17は、ホストマスタ鍵格納部11に格納されている現在のマスタ鍵M・KAによってマスタ鍵N・KBを暗号化したマスタ鍵NデータE(KA, KB)を、端末2を介してICカード3に送信する。その後、ホストマスタ鍵更新手段18によって、ホストマスタ鍵格納部11に格納されている現在のマスタ鍵M・KAをマスタ鍵N・KBに更新することで、次の暗号通信の際はこのマスタ鍵N・KBがマスタ鍵M・KAとなる。

【0021】一方、ICカード3側では、マスタ鍵復元手段19が受信したマスタ鍵NデータE(KA, KB)をICカードマスタ鍵格納部12に格納されているマスタ鍵M・KAにより復号化して、マスタ鍵N・KBを復元する。その後、ICカードマスタ鍵更新手段20によって、ICカードマスタ鍵格納部12に格納されている現在のマスタ鍵M・KAをマスタ鍵N・KBに更新することで、次の暗号通信の際はこのマスタ鍵N・KBがマスタ鍵M・KAとなる。

【0022】ここで、このシステムの安全性について説明する。従来例の場合と同様に、端末2とICカード3

間は安全であるが、ホストコンピュータ1と端末2間には非安全であることを前提としている。ホストコンピュータ1と端末2間で伝送されるマスタ鍵NデータE(KA, KB)、セッション鍵データE(KA, KS)、秘密情報データE(KS, SI)を不正者が全て盗聴し、さらにICカード3を盗んだとする。この不正者がICカード3の暗証番号を知った場合、盗聴したデータをICカード3に入力し、何らかの出力をICカード3から得ることができるが、ICカード3に格納されているマスタ鍵はもはや以前のマスタ鍵M・KAではなく、マスタ鍵N・KBに更新されているため、不正者が欲するセッション鍵KSあるいは秘密情報SIを得ることはできない。

【0023】すなわち、盗聴したマスタ鍵NデータE(KA, KB)をマスタ鍵復元手段14に入力しても、ICカードマスタ鍵格納部12に格納されている鍵は、既にマスタ鍵M・KAではなくマスタ鍵N・KBであるため、何ら意味のあるデータを復元することはできない。

【0024】同様に、盗聴したセッション鍵データE(KA, KS)をセッション鍵復元手段15に入力しても、ICカードマスタ鍵格納部12に格納されている鍵は、既にマスタ鍵M・KAではなくマスタ鍵N・KBであるため、何ら意味のあるデータを復元することはできない。

【0025】なお、セッション鍵KSを復元した時点と、そのために使用したマスタ鍵M・KAからマスタ鍵N・KBへと更新するまでの時点との間が短時間であればあるほど、不正者がセッション鍵データE(KA, KS)を盗聴してICカード3に入力して情報を得る可能性が減少し、安全性は高くなるので好ましいことは言うまでもない。

【0026】(実施の形態2)図2は本実施の形態における暗号通信システムの構成図であり、ホストコンピュータ31と端末32間で秘密暗号鍵を用いて暗号通信を行う場合を示している。

【0027】同図において、ホストコンピュータ31はホストマスタ鍵格納部41に現在のマスタ鍵M・KAを有している。もう一方の復号化のためのマスタ鍵M・KAを端末32内に格納すると、端末32からマスタ鍵M・KAが盗まれる可能性があるため、物理的に安全なICカード33のICカードマスタ鍵格納部42内に格納されている。

【0028】暗号通信の手順を順を追って説明する。まずホストコンピュータ31はマスタ鍵N・KBを生成する。マスタ鍵暗号手段43は、ホストマスタ鍵格納部41に格納されている現在のマスタ鍵M・KAによってマスタ鍵N・KBを暗号化したマスタ鍵NデータE(KA, KB)を、端末32を介してICカード33に送信する。その後、ホストマスタ鍵更新手段44により、ホ

ストマスタ鍵格納部41に格納されている現在のマスタ鍵M・KAをマスタ鍵N・KBに更新し、次の暗号通信の際はこのマスタ鍵N・KBがマスタ鍵M・KAとなる。

【0029】一方、ICカード33側では、マスタ鍵復元手段45が受信したマスタ鍵NデータE(KA, KB)を、ICカードマスタ鍵格納部42に格納されている現在のマスタ鍵M・KAにより復号化してマスタ鍵N・KBを復元する。その後、ICカードマスタ鍵更新手段46により、ICカードマスタ鍵格納部42に格納されている現在のマスタ鍵M・KAをマスタ鍵N・KBに更新する。ここで述べたホストコンピュータ31およびICカード33のマスタ鍵Mの配送および更新は、以下に記述するセッション鍵の配送毎に行うものとする。

【0030】ホストコンピュータ31はセッション鍵KSをランダムに生成する。セッション鍵暗号手段47は、ホストマスタ鍵格納部41に格納されているマスタ鍵N・KBによりセッション鍵KSを暗号化したセッション鍵データE(KB, KS)を、端末32を介してICカード33に送る。ICカード33のセッション鍵復元手段48はこの受信したセッション鍵データE(KB, KS)を、ICカードマスタ鍵格納部42に格納されているマスタ鍵N・KBにより復号化してセッション鍵KSを復元し、これを端末32へ送る。

【0031】これにより、ホストコンピュータ31と端末32は同じセッション鍵KSを共有したこととなり、このセッション鍵KSを用いて暗号通信を行う。具体的には、ホストコンピュータ31の秘密情報暗号手段49がセッション鍵KSにより秘密情報SIを暗号化した秘密情報データE(KS, SI)を生成して端末32に送り、端末32の秘密情報復元手段50がこの秘密情報データE(KS, SI)をセッション鍵KSにより復号化し、秘密情報SIを復元する。そして復元された秘密情報SIにより様々な処理を行うものである。

【0032】ここで、このシステムの安全性について説明する。従来例の場合と同様に、端末32とICカード33間は安全であるが、ホストコンピュータ31と端末32間は非安全であることを前提としている。ホストコンピュータ31と端末32間で伝送されるマスタ鍵NデータE(KA, KB)、セッション鍵データE(KB, KS)、秘密情報データE(KS, SI)を不正者が全て盗聴し、さらにICカード33を盗んだとする。この不正者がICカード33の暗証番号を知った場合、盗聴したデータをICカード33に入力し、何らかの出力をICカード33から得ることができるが、ICカード33に格納されているマスタ鍵はもはや以前のマスタ鍵M・KAではなく、マスタ鍵N・KBに更新されているため、不正者が欲するセッション鍵KSあるいは秘密情報SIを得ることはできない。すなわち、盗聴したデータE(KA, KB)をマスタ鍵復元手段45に入力して

も、ICカードマスタ鍵格納部42に格納されている鍵は、既にマスタ鍵M・KAではなくマスタ鍵N・KBであるため、何ら意味のあるデータを復元することはできない。

【0033】ただし、もしマスタ鍵復元手段45とセッション鍵復元手段48および秘密情報復元手段50が同じアルゴリズムを用いて復号化する場合、次のような手段で秘密データの取得が可能となる。すなわち盗聴したセッション鍵データE(KB, KS)をマスタ鍵復元手段45に入力すると、ICカードマスタ鍵格納部42に格納されている鍵はマスタ鍵N・KBであるため、マスタ鍵復元手段45はセッション鍵KSを出力する。ここで、盗聴した秘密情報データE(KS, SI)をセッション鍵復元手段48に入力すれば、セッション鍵復元手段48はSIを出力してしまう。

【0034】これを防止するためには、単にマスタ鍵復元手段45とセッション鍵復元手段48とに異なるアルゴリズムを採用することである。そうすれば、盗聴したセッション鍵データE(KB, KS)をマスタ鍵復元手段45に入力しても、本来セッション鍵E(KB, KS)はセッション鍵復元手段48により復号化されるべきデータであるため、何ら意味のあるデータを復元することはできない。同様に、セッション鍵復元手段48と秘密情報復元手段50とに異なるアルゴリズムを採用する方法によっても解決できる。

【0035】なお上記各実施の形態においては、暗号・復元化手段や更新手段および格納部を別々の構成としているが、複数の手段をまとめた構成としても同等の効果が得られることは言うまでもない。

【0036】

【発明の効果】以上のように本発明によれば、マスタ鍵によりセッション鍵を暗号化して配送する毎に、マスタ鍵Mをマスタ鍵Nに更新することで、セッション鍵およびそれによって暗号化された秘密情報の不正な解読を防ぐことが可能となるICカードおよびそれを用いた暗号通信システムを提供できる。

【図面の簡単な説明】

【図1】本発明の実施の形態1の暗号通信システムの構成図

【図2】本発明の実施の形態2の暗号通信システムの構成図

【図3】従来の暗号通信システムの構成図

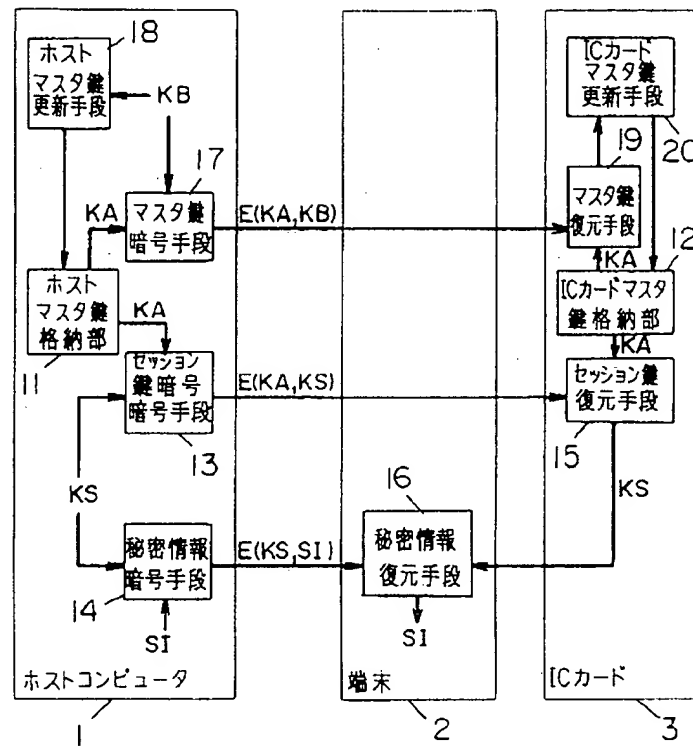
【符号の説明】

- 1、31 ホストコンピュータ
- 2、32 端末
- 3、33 ICカード
- 11、41 ホストマスタ鍵格納部
- 12、42 ICカードマスタ鍵格納部
- 13、47 セッション鍵暗号手段
- 14、49 秘密情報暗号手段

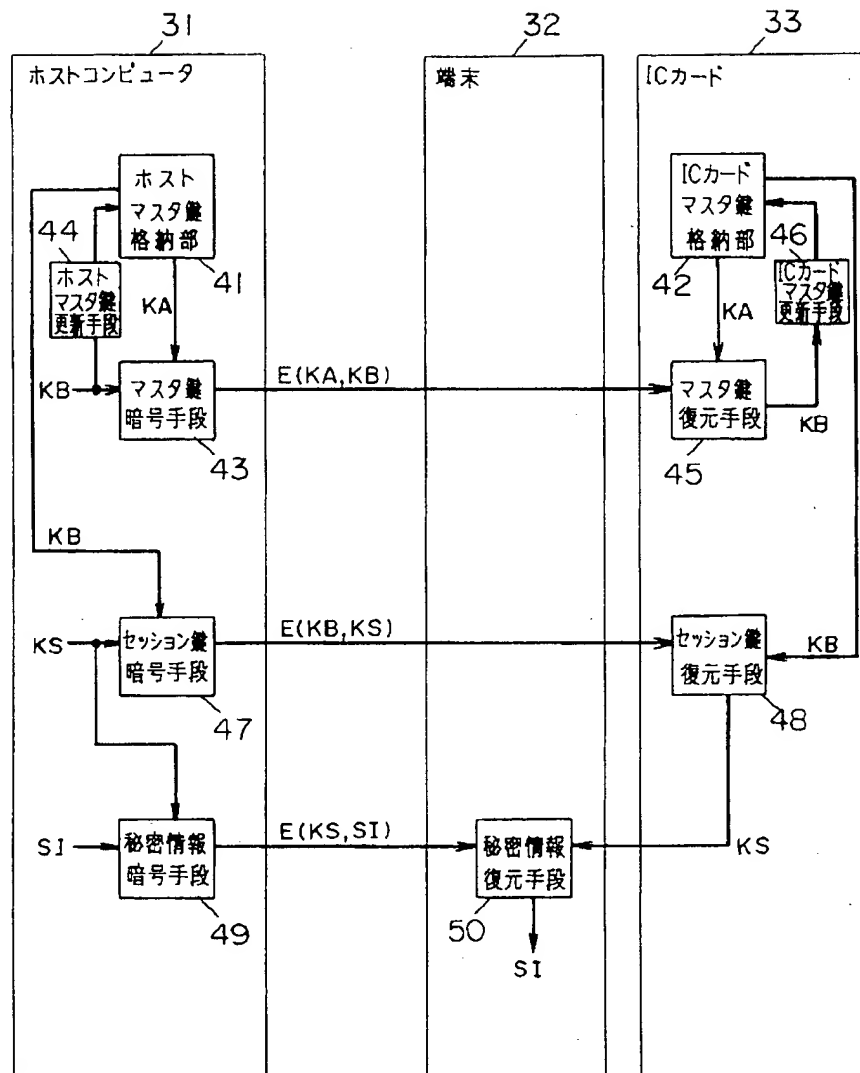
10

- 18、44 ホストマスタ鍵更新手段
19、45 マスタ鍵復元手段
20、46 ICカードマスタ鍵更新手段

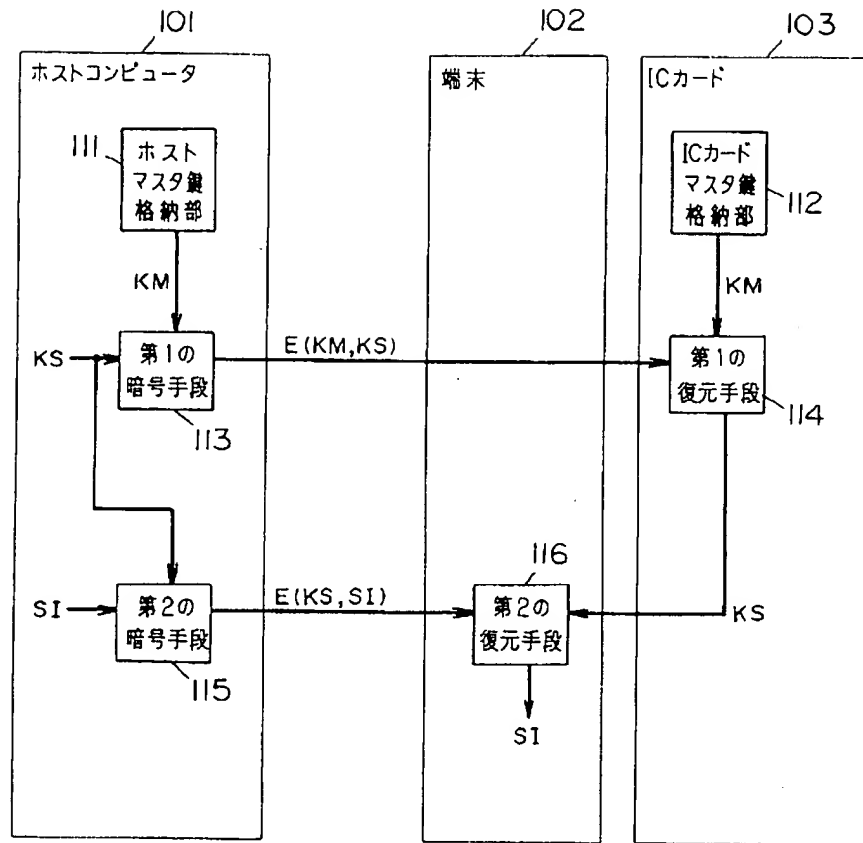
【図 1】



【図2】



【図3】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H 0 4 L 9/00

6 2 1 A